

User Management & Directory Service

Shen Wei

Faculty of Informatics
Technische Universität München

May 28, 2013

Overview

- Linux permission model
- User management
 - Lightweight Directory Access Protocol(LDAP)
 - Pluggable authentication modules (PAM)

Linux permission model

- Linux is **multi-user** system
 - Can the behaviour of one user affect others?
 - How to distribute resources for users?
 - What does a user can and can not do?
- Separate users in groups

Users and groups

- /etc/passwd

```
wei:x:1029:500:Shen Wei,,,:/home/wei:/bin/bash  
login name:password:UID:GID:comments:home:shell
```

- /etc/shadow

```
wei:encrypted password:15597:0:99999:7:::  
login name:password:change date:min age:max age:warning period:inactivity  
period:account expiration:reserved
```

- /etc/group

```
scanner:x:105:saned,wei  
group name:encrypted password:GID:group members
```

Filesystem permissions

- permission triplex: **rwx**
- octal representation

Permission	r	w	x	
---	0	0	0	0
r--	1	0	0	4
rw-	1	1	0	6
rwX	1	1	1	7
...

- permissions for user, group and all

```
-rw-r--r-- 1 shen shen 3184 Apr 10 2010 .bashrc
```

- **chown** and **chmod**

User management

- Manually edit `/etc/passwd` etc.
(If you know what are doing)
- Command-line tools
 - `adduser` and `deluser`
 - `addgroup` and `delgroup`
 - `passwd`, `usermod` and `groupmod`
- User management for the lab group or a company?
 - Phone book
 - Directory service

Directory service

A service for **storing**, **organizing** and **providing access** of information in a directory.

Directory

A database for reading, searching and lookup functions.

- optimized for read operations
- descriptive, attribute-based
- use **scheme** to describe complex data types
- different to database management system
(no roll-back, complicate transactions)



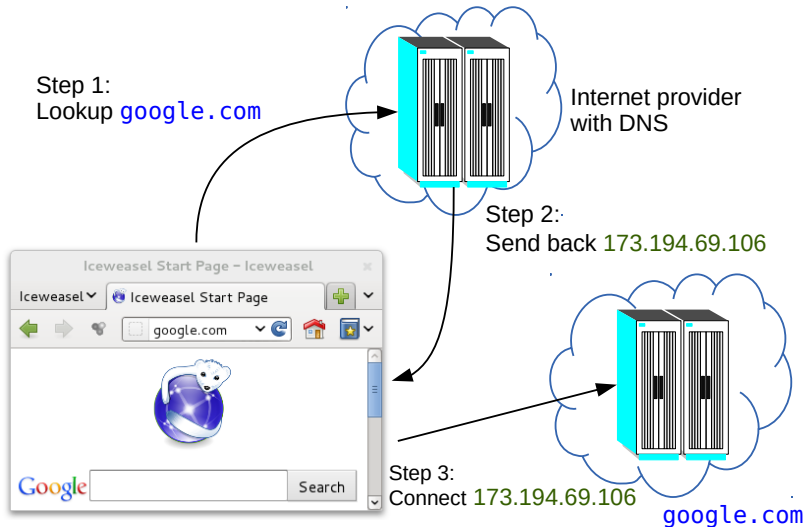
Domain name service

- domain name and IP address
- We know: Visit “Doctor Google” at google.com
- We don't know: What stands behind 173.194.69.106
- Computer knows: How to reach 173.194.69.106
- Computer doesn't understand google.com

Mapping from domain name to IP address?

Domain name service

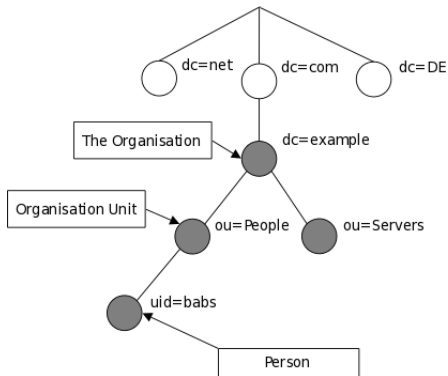
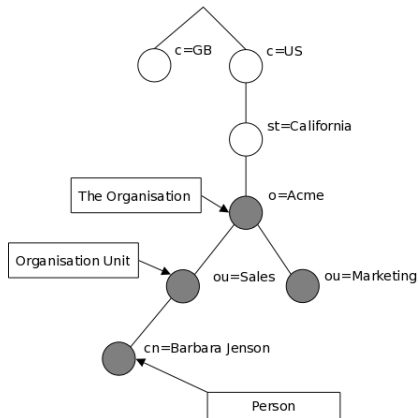
How our computer finds google.



Lightweight Directory Access Protocol

Protocol for **accessing, maintaining** directory information over IP network.

How is the information arranged?



LDIF Format

LDAP Data Interchange Format (LDIF):
representation of **directory entries** and **changes** in text format.

General structure:

```
dn: <distinguished name>  
<attrdesc>: <attrvalue>  
<attrdesc>: <attrvalue>  
<attrdesc>:: <base64-encoded-value>  
<attrdesc>:< <URL>  
...
```

LDIF entry record

```
dn: cn=Shen Wei,dc=tbl  
cn: Shen Wei  
cn: 魏申  
objectclass: person  
description:< file:///tmp/shenwei.txt  
sn: Shen
```

- cn: Common name
- dc: Domain component
- sn: Surname
- Unicode characters are supported

LDIF change record

dn: <distinguished name>

changetype: <[modify|add|delete|modrdn]>

An example:

dn: cn=Shen Wei,dc=tbl

changetype: modify

add: sn

sn: 申

-

replace: description

description: A student

-

Directory service and user management

- LDAP provides name service
- More advanced
 - Builds up complex relationships
 - e.g. employee, office, telephone, login account etc.
- **Scheme(schema)** define different data structures

In schema **nis**:

- posixAccount: defines a POSIX user account
- posixGroup: defines a POSIX user group

Pluggable authentication modules (PAM)

Provide dynamic authentication for applications.

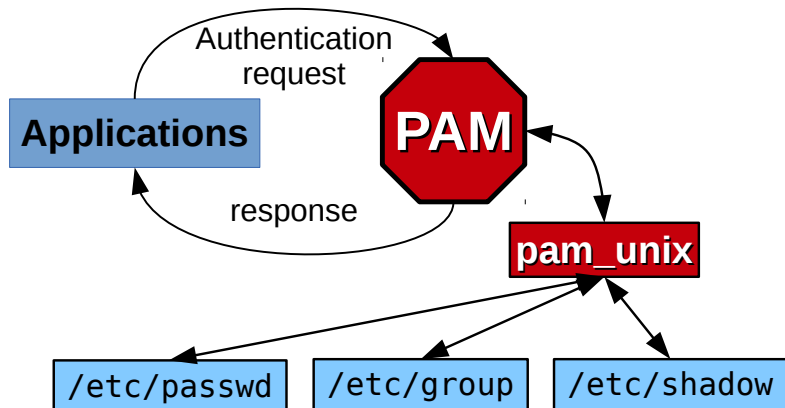
Main components:

- Account module
 - validity of accounts
- Authentication module
 - verification of user's identity
- Password module
 - generation and updating passwords
- Session module
 - definition of actions at beginning and end of sessions

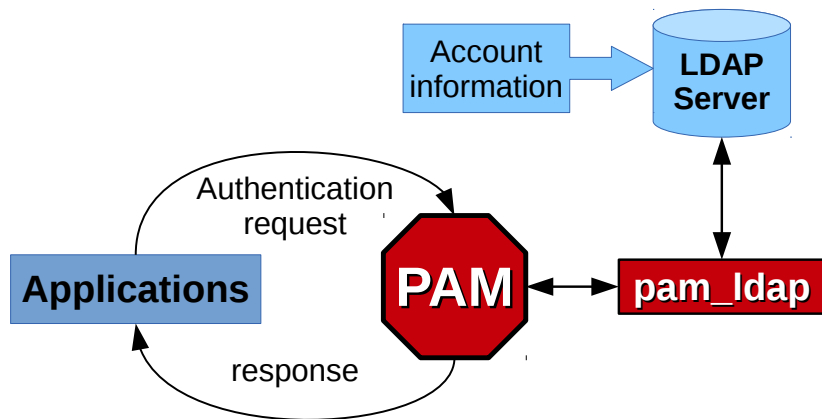
PAM authentication with LDAP

- use LDAP for name service
 - user accounts, user groups, passwords etc.
 - apt-get install libnss-ldap
- update PAM with pam-auth-update
 - load ldap module for PAM
- Use both: **traditional** and **LDAP** authentication model
 - Configuration for name service switch (/etc/nsswitch.conf)
passwd: files ldap
group: files ldap
shadow: files ldap

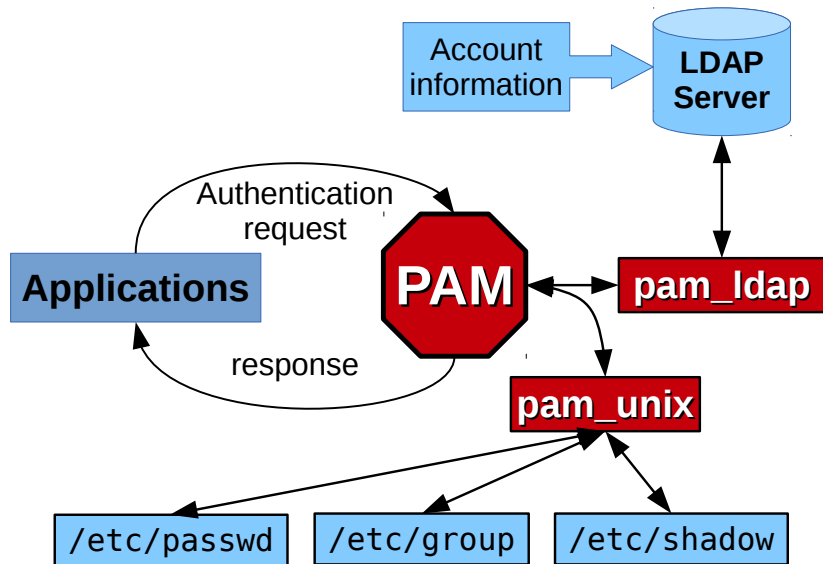
Local authentication model



Authentication using PAM and LDAP



Mixed authentication model



Maintaining LDAP server

Configurations are hardcoded here:

`/etc/ldap/slapd.d/cn=config`

Old plain text configuration file is deprecated.

- Command-line tools for runtime configuration
 - `slapacl`: access control of roles in SLAPD database
 - `slapadd`: add entries in SLAPD database
 - `slapauth`: authentication management in SLAPD database
 - `slapcat`: dump SLAPD database to LDIF file
 - and `slapdn`, `slapindex`, `slaptest`

Access control

- Different data with different sensitivity
- Who can access what information?
- What permission does a user have?

Dynamic access control

- `olcAccess` attribute describes access permissions
- use `slapd` tools such as `slapac1` for modification

Access control attribute:

```
olcAccess: to <what>  
          [by <who> <access> <control>]+
```

Example:

- allow administrator to manage SLAPD database
- break access of others

```
olcAccess: {0}to *  
by dn.exact=gidNumber=0+uidNumber=0,  
cn=peercred,cn=external,cn=auth manage  
by * break
```

Thank you! :)

References

- LPI certification 101 exam prep, Part 3: Intermediate administration, Section: The Linux permissions model
<http://linux.ictlab.kyamk.fi/lpi/1-lpi3/1-lpi3-a4.pdf>
- Wikipedia: Directory Service
http://en.wikipedia.org/wiki/Directory_service
- The OpenLDAP Project
<http://www.openldap.org/project/>
- Wikipedia: LDAP
http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
- Ubuntu Server Guide: OpenLDAP server
<https://help.ubuntu.com/12.10/serverguide/openldap-server.html>
- Pluggable Authentication Modules (PAM)
<http://en.wikipedia.org/wiki/PAM>